



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/711,323	11/09/2000	Alfonso de Jesus Valdes	10454-014002	6879

52197 7590 02/16/2007
PATTERSON & SHERIDAN, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

EXAMINER

MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
----------	--------------

2131

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

09/711,323

Applicant(s)

VALDES ET AL.

Examiner

Aravind K. Moorthy

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 November 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5 and 10-13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5 and 10-13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 November 2000 is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the amendment filed on 15 November 2006.
2. Claims 1-5 and 10-13 are pending in the application.
3. Claims 1-5 and 10-13 have been rejected.
4. Claims 6-9 have been cancelled.

Response to Arguments

5. Applicant's arguments with respect to claims 1-5 and 10-13 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. **Claims 10, 12 and 13 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.**

Independent claim 10 is directed towards a computer readable medium containing an executable program for correlating a first sensor to a second sensor in an intrusion detection system. Independent claim 12 is directed towards a computer readable medium containing an executable program for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised. Independent claim 13 is directed towards a computer readable medium containing an executable program for enhancing the sensitivity of an intrusion detection system that monitors a plurality of computer system resources. When nonfunctional descriptive material is recorded on some computer-readable medium, in a computer or on an electromagnetic carrier signal, it is not statutory since no requisite

Art Unit: 2131

functionality is present to satisfy the practical application requirement. Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored in a computer-readable medium, in a computer, on an electromagnetic carrier signal does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer."). Such a result would exalt form over substance. In *re Sarkar*, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978) ("[E]ach invention must be evaluated as claimed; yet semantogenic considerations preclude a determination based solely on words appearing in the claims. In the final analysis under Sec. 101, the claimed invention, as a whole, must be evaluated for what it is.") (quoted with approval in *Abele*, 684 F.2d at 907, 214 USPQ at 687). See also *In re Johnson*, 589 F.2d 1070, 1077, 200 USPQ 199, 206 (CCPA 1978) ("form of the claim is often an exercise in drafting").

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1-5 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Independent claim 1 has been amended to include the limitations "directly monitored by the second sensor" and "directly monitored by the first sensor". Independent claim 4 has been

Art Unit: 2131

amended to include the limitations “resource directly monitored by the second sensor” and “regarding an apparent normal, degraded or compromised state of a resource directly monitored by the first sensor”. Independent claim 5 has been amended to include the limitations of “directly monitored by the second sensor” and “regarding the existence or validity of services supported on computer system resources directly monitored by the first sensor”. After careful review of the specification, the examiner has found no support for any of the newly added limitations.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1, 2, 4, 5 and 10-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Purtell et al U.S. Patent No. 6,950,947 B1.

As to claim 1, Purtell et al discloses a method for correlating a first sensor to a second sensor in an intrusion detection system, the first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor information about the second sensor's belief state, the belief state indicating a state of at least one system resource or service directly monitored by the second sensor [column 5 line 29 to column 7 line 17]; and

(b) adjusting a prior belief state of the first sensor, the belief state indicating a state of at least one system resource or service directly monitored by the first sensor, the adjustment is based at least in part on the second sensor's belief state [column 5 line 29 to column 7 line 17].

As to claim 2, Purtell et al discloses that the first and second sensors are different types of sensors [column 2, lines 48-55].

As to claim 4, Purtell et al discloses a method of reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored by the second sensor [column 5 line 29 to column 7 line 17]; and

(b) adjusting a prior belief state of the first sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored by the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm [column 5 line 29 to column 7 line 17].

As to claim 5, Purtell et al discloses a method of enhancing the sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding the existence or validity of services supported on computer system resources directly monitored by the second sensor [column 5 line 29 to column 7 line 17]; and

(b) adjusting a prior belief state of the first sensor regarding the existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious [column 5 line 29 to column 7 line 17].

As to claim 10, A computer readable medium containing an executable program for correlating a first sensor to a second sensor in an intrusion detection system, the first and second sensors each maintaining belief over a number of possible states of the system, where the program performs the steps of:

(a) transmitting to the first sensor information about the second sensor's belief state, said belief state indicating a state of at least one system resource or service directly monitored by the second sensor [column 5 line 29 to column 7 line 17]; and

(b) adjusting a prior belief state of the first sensor, said belief state indicating a state of at least one system resource or service directly monitored by

the first sensor, the adjustment based at least in part on the second sensor's belief state [column 5 line 29 to column 7 line 17].

As to claim 11, Apparatus for correlating a first sensor to a second sensor in an intrusion detection system, the first and second sensors each maintaining belief over a number of possible states of the system, the apparatus comprising:

(a) means for transmitting to the first sensor information about the second sensor's belief state, said belief state indicating a state of at least one system resource or service directly monitored by the second sensor [column 5 line 29 to column 7 line 17]; and

(b) means for adjusting a prior belief state of the first sensor, said belief state indicating a state of at least one system resource or service directly monitored by the first sensor, the adjustment based at least in part on the second sensor's belief state [column 5 line 29 to column 7 line 17].

As to claim 12, A computer readable medium containing an executable program for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored resource by the second sensor [column 5 line 29 to column 7 line 17]; and

(b) adjusting a prior belief state of the first sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored by the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm [column 5 line 29 to column 7 line 17].

As to claim 13, A computer readable medium containing an executable program for enhancing the sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding the existence or validity of services supported on monitored computer system resources directly monitored by the second sensor [column 5 line 29 to column 7 line 17], and

(b) adjusting a prior belief state of the first sensor regarding the existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious [column 5 line 29 to column 7 line 17].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Purtell et al U.S. Patent No. 6,950,947 B1 as applied to claim 1 above, and further in view of Timm U.S. Patent No. 5,440,498.

As to claim 3, Purtell et al does not teach that the first sensor is a probabilistic sensor.

Timm teaches a probabilistic sensor in intrusion detection systems [column 5, lines 7-46].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Purtell et al so that the first sensor would have been a probabilistic sensor.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Purtell et al by the teaching of Timm because it provides that ability to compare the effectiveness of any security element or group of elements of the security system with another element or group of elements. Not only does this method reveal the less effective security elements of a system, but also it can be employed to evaluate whether proposed additions to a security system would enhance protection of the facility and, if so, by how much [column 2, lines 16-29].

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

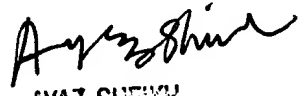
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy 
February 14, 2007


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100